7487

écrit

MATHÉMATIQUES GÉNÉRALES

DURÉE : 6 heures

Les cinq parties du problème sont dépendantes, mais on peut traiter chacune en admettant les résultats de celles qui précèdent.

PREMIÈRE PARTIE

Soient G un groupe fini, noté multiplicativement, n le cardinal de G et e son élément neutre. Si A est un anneau commutatif unitaire, d'unité ε, on désigne par A [G] l'ensemble des fonctions de G dans A et on définit dans A [G] deux opérations de la façon suivante :

$$(u + v)(g) = u(g) + v(g)$$

$$(uv)(g) = \sum_{\substack{h,\, k \in G \\ hk = g}} u(h)\, v(k)$$

pour tous u, $v \in$ A [G] et $g \in$ G. On définit enfin $X_g \in$ A [G] par $X_g(h) = \varepsilon$ (resp. 0) si $g = h$ (resp. $g \neq h$).

1° *a.* Montrer que A [G] est un anneau unitaire et que l'application $g \longmapsto X_g$ permet d'identifier, ce qu'on fera désormais, G à un sous-groupe du groupe des éléments inversibles de A [G]. Est-il possible d'identifier, de manière analogue, A à un sous-anneau de A [G] ? Quelle est la condition nécessaire et suffisante pour que A [G] soit commutatif ?

b. Établir que A [G] n'est jamais intègre, sauf dans un cas particulier qu'on précisera.

2° Soit K un corps commutatif de caractéristique nulle.

a. Vérifier que K [G] est muni canoniquement d'une structure de K-espace vectoriel, pour laquelle G est une base de K [G].

b. Pour tout $u \in K[G]$, on note f_u l'application $v \longmapsto uv$ de K [G] dans lui-même et on pose $\theta(u) = \text{trace}(f_u)$. Démontrer que $\theta(u) = n.u(e)$.

c. La forme bilinéaire $(u, v) \longmapsto \theta(uv)$ est-elle symétrique, non dégénérée ?

3° On suppose, dans cette question, que G est abélien et on prend pour K le corps $\mathbb{C}$ des nombres complexes.

a. Démontrer que chaque f_u est diagonalisable, puis qu'il existe une base B de $\mathbb{C}[G]$ dans laquelle chacun des f_u, $u \in \mathbb{C}[G]$, est représenté par une matrice diagonale, de la forme :

$$\begin{pmatrix} \lambda_1(u) & & & 0 \\ & \cdot & & \\ & & \cdot & \\ & & & \cdot \\ 0 & & & \lambda_n(u) \end{pmatrix}$$

b. Établir que l'application $u \longmapsto (\lambda_1(u), \ldots, \lambda_n(u))$ est un isomorphisme de $\mathbb{C}$-algèbres entre $\mathbb{C}[G]$ et $\mathbb{C}^n$.

DEUXIÈME PARTIE

Les notations sont celles de la première partie et on suppose G abélien. P est l'ensemble formé de 1 et de tous les nombres premiers; pour $g \in G$ et $s \in P$, on pose $[g, s] = 1 - g$ (resp. $= 1 + g + g^2 + \ldots + g^{s-1}$) si $s = 1$ (resp. si s est un nombre premier), $[g, s]$ est un élément de $\mathbb{Z}(G)$, $\mathbb{Z}$ désignant l'anneau des entiers relatifs.

1° *a.* Soit $S = \{u_1, \ldots, u_k\}$ une partie finie de $\mathbb{Z}[G]$, montrer qu'il existe un sous-groupe H de G, minimum pour l'inclusion, tel que $S \subset \mathbb{Z}[H]$; lorsque $S \subset G$, vérifier que H est le sous-groupe de G engendré par S. On posera désormais $H = < u_1, \ldots, u_k >$ et on notera $l(u_1, \ldots, u_k)$ la somme de tous les exposants de la décomposition en facteurs premiers de card (H).

b. Soient u un élément non nul de $\mathbb{Z}[G]$ et $(g, s) \in G \times P$ tels que $u[g, s] = 0$; établir que g appartient à $< u >$.

2° On étudie maintenant une équation du type (I) : $u[g_1, s_1] \ldots [g_k, s_k] = 0$, où $u \in \mathbb{Z}[G]$ et $(g_1, s_1), \ldots, (g_k, s_k) \in G \times P$, équation que l'on suppose minimale en ce sens que chacun des k produits obtenus en y omettant l'un des $[g_i, s_i]$ est non nul. On se propose, par récurrence sur le nombre $m = l(g_1) + \ldots + l(g_k)$, de montrer que (I) implique (II), (II) étant la propriété suivante :

$$l(u, g_1, \ldots, g_k) < l(u) + k.$$

a. Prouver le résultat lorsque $l(g_1) + \ldots + l(g_k) = 1$ (on pourra d'abord observer que chacun des $l(g_i)$ est $\geqslant 1$ lorsque $k \geqslant 2$).

b. On suppose désormais l'implication établie pour les valeurs $1, \ldots, m-1$ et que l'équation (I), correspondant au nombre m, est vérifiée. Démontrer qu'alors :

$$l(u[g_1, s_1] \ldots [g_r, s_r], g_{r+1}, \ldots, g_k) < l(u[g_1, s_1] \ldots [g_r, s_r]) + k - r$$

pour $r = 1, \ldots, k-1$.

c. Vérifier que $l(u, g_1, \ldots, g_k) - l(u, g_1, \ldots, g_r) < k - r$ pour $r = 1, \ldots, k-1$ (on pourra d'abord montrer que, si $H \subset K$ sont deux sous-groupes de G et S une partie de G, alors l'indice de $< H \cup S >$ dans $< K \cup S >$ divise celui de H dans K). En déduire la relation (II) dans le cas où l'un des $l(g_i)$ vaut 1.

3° Démontrer (II) dans le cas où tous les $l(g_i)$ sont > 1 (on pourra, dans (I), chercher à remplacer $[g_k, s_k]$ par $[g, 1]$ avec $l(g) = l(g_k) - 1$ et, après simplifications, obtenir une relation du type (I) à laquelle l'hypothèse de récurrence soit applicable).

TROISIÈME PARTIE

G est toujours un groupe abélien fini, mais son opération est maintenant notée additivement, et 0 désigne son élément neutre. Si $S_1, \ldots, S_k$ sont des parties de G, on dit que G est somme directe des S_i, et on note $G = S_1 \oplus \ldots \oplus S_k$ lorsque l'application $(g_1, \ldots, g_k) \longmapsto g_1 + \ldots + g_k$ de $S_1 \times \ldots \times S_k$ dans G est bijective. Par ailleurs, on appelle période de la partie $S \subset G$ tout élément $g \in G - \{0\}$ tel que $g + S = S$; S est dite périodique lorsqu'elle a au moins une période. Enfin, on appelle arc toute partie de G de la forme $[g]_q = \{0, g, \ldots, (q-1)g\}$ avec $g \in G$ et $1 < q \leqslant \text{ordre}(g)$.

1° *a.* Vérifier qu'un arc est périodique si, et seulement si, c'est un sous-groupe cyclique de G.

b. Montrer qu'une partie $S \subset G$ est périodique si, et seulement si, il existe $g \in G - \{0\}$ et $S' \subset G$ tels que $S = \langle g \rangle \oplus S'$.

c. En déduire que, pour tout arc S, on peut trouver une décomposition de la forme :

$$S = [g_1]_{p_1} \oplus \ldots \oplus [g_r]_{p_r}$$

$p_1, \ldots, p_r$ étant des nombres premiers, ayant en outre la propriété que les conditions « S est un sous-groupe de G » et « l'un des $[g_i]_{p_i}$ est un sous-groupe de G » soient équivalentes.

2° On se propose de démontrer que, si $G = [g_1]_{k_1} \oplus \ldots \oplus [g_r]_{k_r}$, alors au moins l'un des $[g_i]_{k_i}$ est un sous-groupe de G.

a. Vérifier qu'on ne restreint pas la généralité en supposant, pour prouver ce résultat, que chaque k_i est un nombre premier p_i.

b. Soient $p_1, \ldots p_r$ des nombres premiers et $g_1, \ldots g_r$ des éléments de G, tels que $G = [g_1]_{p_1} \oplus \ldots \oplus [g_r]_{p_r}$ et que $[g_r]_{p_r}$ ne soit pas un sous-groupe de G; on pose $g = p_r g_r$ et, pour toute partie I de $\{1, \ldots, r\}$, $S_I = \bigoplus_{i \in I} [g_i]_{p_i}$.

Vérifier que g est non nul et que $S_{\{1, \ldots, r-1\}}$ est g-périodique; en déduire qu'il existe une partie $J \subset \{1, \ldots, r-1\}$ telle que S_J soit g-périodique mais qu'aucun des $S_{J'}$, pour J' inclus strictement dans J, ne le soit.

c. Quitte à renuméroter $g_1, \ldots, g_{r-1}$, on suppose que $J = \{1, \ldots, k\}$, avec $1 \leqslant k \leqslant r-1$, et on pose $H = \langle g_1, \ldots, g_k \rangle$. Montrer que $p_1 \ldots p_k$ divise card (H).

3° Démontrer que $l(g_1, \ldots, g_k) \leqslant k$ (on pourra, en revenant à la notation multiplicative, appliquer la seconde partie); en déduire, par récurrence sur r, le résultat cherché.

QUATRIÈME PARTIE

Pour tous $n \geqslant 1$ et $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, on pose $\|x\| = \sqrt{x_1^2 + \ldots + x_n^2}$ et $\|x\|_\infty = \max(|x_1|, \ldots, |x_n|)$; $(\,|\,)$ désigne le produit scalaire associé à $\|\ \|$.

Si K est une partie compacte de $\mathbb{R}^n$, on note $\mu(K)$ son volume (au sens de la mesure de Lebesgue) et on pose $v_n = \mu(\{x \in \mathbb{R}^n / \|x\| \leqslant 1\})$. On rappelle enfin que $GL(n, \mathbb{Z})$ est le groupe multiplicatif formé de toutes les matrices $A \in M_n(\mathbb{Z})$ qui sont inversibles dans $M_n(\mathbb{Z})$.

On appelle réseau de $\mathbb{R}^n$ toute partie $L \subset \mathbb{R}^n$ qui possède les deux propriétés suivantes :

i. L est un sous-groupe additif de $\mathbb{R}^n$ et n'est contenu dans aucun hyperplan;

ii. La topologie induite dans L par $\mathbb{R}^n$ est discrète.

Si L est un réseau et K un compact de $\mathbb{R}^n$ contenant 0, on dit que K est L-entassable (resp. L–couvrant) lorsque les $a + K$, a décrivant L, ont des intérieurs deux à deux disjoints (resp. recouvrent $\mathbb{R}^n$); K est appelé L–pavé lorsqu'il est à la fois L–entassable et L–couvrant.

1° *a.* Vérifier que la condition *ii.* ci-dessus est équivalente à chacune des deux suivantes :

iii. Toute suite convergente d'éléments de L est constante à partir d'un certain rang.

iv. Pour toute partie bornée Ω de $\mathbb{R}^n$, $\Omega \cap L$ est un ensemble fini.

b. Démontrer que tout réseau L a une $\mathbb{Z}$–base, c'est-à-dire une base $B = (e_1, \ldots, e_n)$ de $\mathbb{R}^n$ telle que $L = \mathbb{Z}\, e_1 \oplus \ldots \oplus \mathbb{Z}\, e_n$, et que, si $B' = (e'_1, \ldots, e'_n)$ est une base de $\mathbb{R}^n$, c'est une $\mathbb{Z}$-base de L si, et seulement si, la matrice de passage de B à B′ appartient à $GL(n, \mathbb{Z})$.

c. Avec les notations du *b.*, on pose :

$$K_0 = \{ t_1 e_1 + \ldots + t_n e_n \mid t_1, \ldots, t_n \in [0, 1] \}$$

et S désigne la matrice carrée d'ordre n dont l'élément (i, j) est $(e_i \mid e_j)$. Montrer que K_0 est un L–pavé, que $\mu(K_0) = \sqrt{\det(S)}$ et que cette dernière quantité est indépendante de la $\mathbb{Z}$–base choisie, on la notera désormais $\mu(L)$.

2° L étant un réseau de $\mathbb{R}^n$, pour tout réel $a > 0$, on note $N_L(a)$ le nombre d'éléments de L qui vérifient la relation $\| x \|_\infty \leqslant a$.

a. Démontrer que $(2a)^n / N_L(a)$ tend vers $\mu(L)$ quand a tend vers $+\infty$ (on pourra utiliser un L–pavé); en déduire que, si K est L–entassable (resp. L–couvrant), alors $\mu(K) \leqslant \mu(L)$ (resp. $\mu(K) \geqslant \mu(L)$).

b. Inversement, on suppose que K est, soit L–entassable, soit L–couvrant; prouver que K est un L–pavé si, et seulement si, $\mu(K) = \mu(L)$.

c. Soit L′ un sous-groupe de L, qui soit également un réseau de $\mathbb{R}^n$; démontrer que l'indice de L′ dans L est fini et qu'en notant P la matrice de passage d'une $\mathbb{Z}$–base de L à une $\mathbb{Z}$–base de L′, on a :

$$[L : L'] = \frac{\mu(L')}{\mu(L)} = |\det(P)|.$$

3° L est toujours un réseau de $\mathbb{R}^n$.

a. Soit C un compact de $\mathbb{R}^n$, convexe et symétrique par rapport à 0, tel que $\mu(C) > 2^n \mu(L)$, montrer que C contient au moins un élément non nul de L.

b. Étendre cette propriété au cas où $\mu(C) = 2^n \mu(L)$ et en conclure qu'il existe un $x \in L$ tel que $0 < \| x \| \leqslant 2 \left(\sqrt[n]{\mu(L) / v_n}\right)$.

4° On suppose, dans cette question seulement, que $n = 4$.

a. Soit p un nombre premier impair, montrer qu'il existe α et $\beta \in \mathbb{Z}$ tels que $\alpha^2 + \beta^2 + 1 \equiv 0\,[p]$.

b. On pose $L = \{ (a, b, c, d) \in \mathbb{Z}^4 \mid \alpha a + \beta b \equiv c\,[p] \text{ et } \alpha b - \beta a \equiv d\,[p] \}$, établir que L est un réseau de $\mathbb{R}^4$ et calculer $[\mathbb{Z}^4 : L]$; en déduire qu'il existe $a, b, c, d \in \mathbb{Z}$ tels que $0 < a^2 + b^2 + c^2 + d^2 < 2p$, puis que $a^2 + b^2 + c^2 + d^2 = p$.

c. Démontrer que tout nombre entier naturel est la somme de quatre carrés d'entiers.

CINQUIÈME PARTIE

On note $(u_1, \ldots, u_n)$ la base canonique de $\mathbb{R}^n$ et Δ le « cube » formé de tous les $t_1 u_1 + \ldots + t_n u_n$, pour $t_1, \ldots, t_n \in [0, 1]$. Si L est un réseau tel que Δ soit un L–pavé, on dit que (Δ, L) est un pavage par piles lorsque l'un des u_i appartient à L, et un pavage décalé dans le cas contraire.

Le but du problème est de montrer que tout pavage de $\mathbb{R}^n$ est un pavage par piles.

1° Soit L un réseau de $\mathbb{R}^n$ tel que Δ soit un L–pavé (on dira simplement Δ–réseau par la suite), prouver que l'intérieur de Δ est disjoint de L et que $\mu(L) = 1$; ces deux conditions impliquent-elles inversement que L est un Δ–réseau ?

2° Soit L un Δ–réseau dont tous les points ont leurs composantes rationnelles, c'est-à-dire tel que $L \subset \mathbb{Q}^n$.

a. Montrer qu'il existe un entier $q \geqslant 1$ tel que $qL \subset \mathbb{Z}^n$; combien vaut $[\mathbb{Z}^n : qL]$?

b. On note G le groupe-quotient $\mathbb{Z}^n / qL$ et $g_1, \ldots, g_n$ les images canoniques dans G de $u_1, \ldots, u_n$. Démontrer qu'avec les notations de la troisième partie on a

$$G = [g_1]_q \oplus \ldots \oplus [g_n]_q .$$

c. En déduire que (Δ, L) est un pavage par piles.

3° On se propose d'étendre à un Δ–réseau quelconque le résultat du 2°; raisonnant par l'absurde, on suppose qu'il existe un Δ–réseau L tel que (Δ, L) soit un pavage décalé et, quitte à renuméroter les u_i, qu'au moins un élément de L a sa première composante irrationnelle.

a. Établir qu'il existe une $\mathbb{Z}$–base $(\varepsilon_1, \ldots, \varepsilon_n)$ de L et un entier $i \geqslant 1$ tels que les éléments de L dont la première composante est rationnelle soient exactement ceux de $\mathbb{Z}\,\varepsilon_1 \oplus \ldots \oplus \mathbb{Z}\,\varepsilon_{i-1}$. Pour tout $t = (t_i, \ldots, t_n) \in \mathbb{R}^{n-i+1}$, on note L_t le sous-groupe de $\mathbb{R}^n$ engendré par $(\varepsilon_1, \ldots, \varepsilon_{i-1}, \varepsilon_i + t_i u_1, \ldots, \varepsilon_n + t_n u_1)$; prouver que L_t est un réseau pour t suffisamment petit et qu'alors Δ est L_t–entassable.

b. Démontrer que L_t est un Δ–réseau pour tout $t \in \mathbb{R}^{n-i+1}$.

c. Démontrer qu'il existe un t tel que (Δ, L_t) soit décalé et que tous les éléments de L_t aient leur première composante rationnelle.

d. En déduire qu'il existe un Δ–réseau décalé inclus dans $\mathbb{Q}^n$ et conclure.